Google

Buying Spying

Insights into Commercial Surveillance Vendors

Executive Summary

The commercial surveillance industry has emerged to fill a lucrative market niche: selling cutting edge technology to governments around the world that exploit vulnerabilities in consumer devices and applications to surreptitiously install spyware on individuals' devices. By doing so, commercial surveillance vendors (CSVs) are enabling the proliferation of dangerous hacking tools.

The harm is not hypothetical. Spyware vendors point to their tools' legitimate use in law enforcement and counterterrorism. However, spyware deployed against journalists, human rights defenders, dissidents, and opposition party politicians — what Google refers to as 'high risk users' — has been well documented, both by analysis from Google, and by researchers from organizations like the University of Toronto's Citizen Lab and Amnesty International. While the number of users targeted by spyware is small compared to other types of cyber threat activity, the follow-on effects are much broader. This type of focused targeting threatens freedom of speech, a free press, and the integrity of elections worldwide.

As threat actors, CSVs pose a threat to Google users, as half of known 0-day exploits used against Google products, as well as Android ecosystem devices, can be attributed to CSVs. Google takes the security of our users very seriously, with dedicated teams in place to protect against attacks from a wide range of sources. Today, Google's Threat Analysis Group (TAG) actively tracks around 40 CSVs, with varying levels of sophistication and public exposure, selling exploits and surveillance capabilities to government customers.

In the appendix of this report, we have included an overview of a subset of the CSVs tracked by Google, their products, and the exploits they use against consumer devices and applications.

This report outlines our understanding of who is involved in developing, selling, and deploying spyware, how CSVs operate, the types of products they develop and sell, and analysis of recent activity. Our report includes the following observations:

- **First, while prominent CSVs like NSO Group garner public attention and headlines, there are dozens of smaller CSVs, as well as other important parts of the exploitation supply chain, which play an important role in the development of spyware.** All these players enable the proliferation of dangerous tools and capabilities used by governments against individuals, which threatens the safety of the Internet ecosystem and the trust on which a vibrant and inclusive digital society depends.
- **Second, CSV tools are used against journalists, human rights defenders, dissidents, and political opponents.** High risk users we spoke with attested to the fear felt when these tools are used against them, the chilling effect on their professional relationships, and their determination to continue their important work.
- **Third, if governments ever had a monopoly on the most sophisticated capabilities, that era is certainly over. The private sector is now responsible for a significant portion of the most sophisticated tools we detect.** In 2023, TAG discovered 25 0-days being actively exploited in-the-wild, 20 of which were exploited by CSVs.
- **Finally, CSVs pose a threat to Google users, and Google is committed to disrupting that threat and keeping our users safe.** CSVs are behind half of known 0-day exploits targeting Google products as well as Android ecosystem devices. Of the 72 known in-the-wild 0-day exploits affecting Google products since mid-2014, TAG attributes 35 of these 0-days to CSVs. This is a lower bounds estimate, as it reflects only known 0-day exploits where we have high confidence in attribution. The actual number of 0-days developed by CSVs is almost certainly higher, including 0-days targeting Google products.

We hope this report will serve as a call to action. As long as there is a demand from governments to buy commercial surveillance technology, CSVs will continue to develop and sell spyware. We believe it is time for government, industry and civil society to come together to change the incentive structure which has allowed these technologies to spread so widely.

Google is committed to leading the industry in detecting and disrupting these threats, with a long track record combating commercial surveillance tools targeting our users. In 2017 Google's Android was the first mobile platform to warn users about NSO Group's Pegasus spyware. They released research, remediated the compromise, and implemented controls against a newly discovered family of spyware, called Chrysaor at the time but later known as Pegasus, used in a targeted attack on a small number of Android devices.

Demand from government customers remains strong and our findings underscore the extent to which CSVs have proliferated hacking and spyware capabilities that weaken the safety of the Internet for all. To meet the demand from government customers CSVs find and develop exploits, and have emerged as well-paying customers of exploit developers and brokers, incentivizing exploit sales at the expense of security. TAG strives to continuously improve the safety and security of Google products, share intelligence with our industry peers, and publicly release information about the operations we disrupt.

We are joined in this effort by many other Google security teams:

- Project Zero, security researchers who study zero-day vulnerabilities in hardware and software systems;
- Safe Browsing, which protects over five billion devices by showing warnings to users when they attempt to navigate to dangerous sites or download malicious files;
- Android, Chrome, and other product security teams who quickly detect, disrupt, analyze, and prevent threats against our users;
- Mandiant, now part of Google Cloud, a provider of dynamic cyber defense, threat intelligence and incident response services.

Spyware causes real-world harm

Compared to other cyber threats, spyware is used against a small number of targets. But the use against high risk targets has a profound impact on society. Spyware is often abused by governments for purposes antithetical to a free society including targeting dissidents, journalists, human rights defenders, and opposition party politicians.

What is spyware?

Spyware, also referred to as an implant or agent, is surveillance software that is surreptitiously installed on a device to collect the user's data and send it back to the attacker.

To illustrate the real world harm, TAG partnered with Jigsaw — a unit within Google that explores threats to open societies — to highlight the experiences of three high risk users targeted with Pegagus, a well-known spyware developed by NSO Group. **Their experiences show the disruption and fear caused by spyware, and are a small sample of the victims, CSVs, and tools involved in such incidents.**

María Luisa Aguilar Rodríguez

International Advocacy Officer, Centro PRODH

On Christmas Eve 2022, María Luisa Aguilar Rodríguez of the Mexico City-based human rights organization Centro PRODH received a text message. The automated alert from Apple stated that she had been the target of a government-backed hack. An identical message appeared shortly after in her email. Twelve minutes later, Santiago Aguirre, the organization's director, appeared in her office, having received the same messages. Subsequent forensic analysis by Citizen Lab confirmed both had been targeted by NSO Group's Pegasus spyware — and not for the first time.

> “It was terrifying. We didn’t know how this happened, or what was going to happen next.”

Aguilar Rodríguez and Aguirre believe the hacking is connected to their efforts to bring transparency to what has become known as the Iguala Case dating back to 2014, where a confrontation between police, students, locals and passersby resulted in six people being killed, and 43 students detained by authorities and never seen again. Nine years later, despite tireless efforts of parents, human rights lawyers, journalists and advocates, the ultimate fate of these students remains unknown.

In 2017, Aguirre was in Mexico City listening to the local news on the radio with his partner when he heard a familiar voice — his own. A recently created Facebook account had uploaded audio from phone calls between Aguirre and the father of one of the disappeared students along with another call between a colleague of a partner organization in the case and his wife, heavily edited to make it appear that they were in league with the local cartels. “It was terrifying,” Aguirre says. “We didn’t know how this happened, or what was going to happen next.”

A tip from the Mexican digital human rights organization R3D prompted Aguirre and his colleagues to search their texts for a suspicious URL. Aguirre found two messages, both carefully tailored to appear plausible to him — one from an individual claiming to have a brother who had been arrested for protesting in Guerrero and another from an individual posing as one of his students — containing the malicious links. Subsequent analysis by Citizen Lab would confirm that these links had in fact been used to install Pegasus on his phone along with the phones of two other colleagues.

When Aguirre and Aguilar Rodríguez were hacked in 2022, carefully crafting tailored deceptive messages were no longer needed as a lure: their phones were wholly compromised without them having to take any action at all. “When lawmakers are debating about these tools,” Aguilar Rodríguez says, “maybe there’s some legitimate purpose for them. And maybe they have the institutions and the rules and the oversight to use them safely. But [...] it’s important that they remember that these tools will also be used in places where institutions are very weak, where there are no controls.”

Despite the repeated hacking of her colleagues, Aguilar Rodríguez says it hasn’t changed how she approaches her work. “... we have to put all of our efforts into continuing to search for the students and answering what happened to them.”

Galina Timchenko

Co-founder, CEO, and Publisher of Meduza

Photo credit: Andrej Vasilenko for Monocle

"I wasn't afraid," Galina Timchenko, co-founder and CEO of the exiled Russian media outlet Meduza says of the moment she learned in July that she had been targeted and hacked with Pegasus between February 6 and 26, 2023. The country behind the hacking remains unclear. "In 2012," she says, speaking of the year Vladimir Putin returned to the Russian presidency and the crackdown on independent media in the country ramped up, "I decided I wouldn't do anything on the internet that I wouldn't do openly in front of anyone."

But as the implications of the hacking gradually became clear to her, that began to change. “For weeks they had full access to my correspondence, so they could see my close circle. I was afraid for them. I was afraid for my friends, my colleagues and Meduza’s partners.” Later, sitting for an interview with one of her own reporters who would write up the story of her hacking — the first hacking of a Russian journalist with NSO Group’s Pegasus — the potential consequences would be brought home even more clearly. “‘You know,’ she said to me, ‘several of the reporters who have been hacked with Pegasus have been killed.’ And, ‘oh my god,’ I thought, ‘I do not want to meet the same fate as Khashoggi,” she says, referring to Jamal Khashoggi, the Washington Post reporter assassinated in 2018 whose close associates had also been targeted with Pegasus.

Meduza was founded in Riga, Latvia in 2014, the same year as Russia’s annexation of Crimea. “It was the year Russian propaganda just exploded,” she says. “It had always been there, but it was very dry, very official, very boring. Then it was everywhere — on every show, on every screen.” Meduza sought to counter this hostile takeover of the information environment, combining high quality reporting with a wry sense of humor that quickly drew a large Russian audience.

The hacking of Timchenko’s phone coincided with a meeting of exiled media outlets in Berlin. The meeting had been organized in an attempt to develop a strategy to respond to the massive expansion of Russia’s “foreign agents” laws that had gone into effect in December 2022. According to Human Rights Watch, “the law expands the definition of foreign agent to a point at which almost any person or entity… could be designated a foreign agent, so long as the authorities claim they are under ‘foreign influence.’” Meduza had itself already been declared a foreign agent in April 2021.

Even in the face of escalating risk, Timchenko remains undeterred. “It’s not about me,” she ultimately says of the hacking.

> “It’s not about my safety, my security. This is a threat to anyone with any access to sensitive information, any expertise. No one is safe.”

“There’s still an audience,” she says, of Meduza’s continuing efforts to piece together the new iron curtain of Russian censorship laws. “Russian internet users, our readers, they’re still there — millions of them. And there’s no way we’re leaving them to the jerks in the Kremlin. We have no right.”

Carlos Dada

Co-Founder and Director of El Faro

“This is the part I hate most,” Carlos Dada, co-founder and director of the Salvadoran investigative news outlet El Faro, says of having to discuss the hacking of his and 21 of his colleagues' phones with the Pegasus spyware. “It has drained so many resources from our organization, resources that should be focused on investigating power, political power, economic power.” “But,” he continues, “we have a moral obligation to speak up. We are not the only victims. We’re just the ones with the loudest voice.”

Dada co-founded El Faro with Jorge Simán in 1998, six years after the Chapultepec Peace Accords brought an end to more than a

decade of civil war in El Salvador. Both founders had grown up in exile due to the conflict, returning to El Salvador with a conviction that the country's nascent democracy could only survive with a strong independent media, something that hadn't existed there in decades. "There was no one in El Salvador from whom we could learn, or take the baton from," Dada explains. "We had to learn as we built."

Establishing and sustaining an investigative outlet in a country with little history of independent journalism was never going to be an easy task, but El Faro's dogged reporting on organized crime and government corruption quickly earned it both accolades and powerful opponents. It is perhaps in part due to this history of surveillance and intimidation that when Julia Gavarrete, a reporter for El Faro, began to notice strange behavior on her phone — overheating, apps opening and closing by themselves — she suspected there might be a problem. The digital rights group Access Now connected her with Citizen Lab, who identified traces of Pegasus infection on her phone. Subsequent analysis of more of the staff's phones revealed repeated and sustained infections between June 2020 and November 2021, lasting in the case of one reporter, Carlos Martínez, 269 days.

On January 12, 2022, El Faro reported the results of Citizen Lab's investigations. "We lost all our sources the day we published," Dada says. "We've always done everything we can to protect our sources, but this time it was different, and they needed to know." The publication also forced Dada into exile once again.

In November of last year, Dada along with 14 of his colleagues filed suit against NSO Group in California with the Knight First Amendment Institute, alleging that NSO Group has violated the Computer Fraud and Abuse Act and the California Comprehensive Computer Data Access and Fraud Act, among other laws, in developing Pegasus spyware and deploying it against journalists. Beyond the immediate cause of justice, Dada hopes that the suit will compel NSO Group to divulge the client state that targeted him and his coworkers. Dada explains, "When it is used to attack

journalists we are entitled to know who is using this weapon against us, because it is a weapon."

For Dada, the suit is also a message. "Despite everything they're doing against us, we're not frozen. We're not scared, hiding in a corner. We're determined to keep doing what we're doing."

TAG continues to see CSV tools used in ways that harm not only the targeted individuals, but society at large. The use of spyware against political candidates threatens a society's ability to hold free and fair elections. In 2021, TAG reported on five zero-day vulnerabilities affecting Chrome and Android that, before they were patched, were used to compromise Android users, including journalists and opposition politicians. We assess with high confidence that the CSV Intellexa packaged these vulnerabilities, and sold the hacking software to at least eight governments, including Egypt, Armenia, Greece, Madagascar, Côte d'Ivoire, Serbia, Spain and Indonesia. Our reporting is consistent with earlier analysis produced by Citizen Lab and Meta.

Similar activity continued through 2023. In April, TAG observed two customers of Intellexa using the company's surveillance system in Indonesia and Madagascar using national elections and political candidates as lures. Five months later, in September 2023, TAG and Citizen Lab discovered the Predator spyware from Intellexa targeting an Egyptian opposition politician who had announced his intent to run in the Egypt presidential election.

The spyware industry: understanding CSVs

CSVs sell spyware to government customers, along with the infrastructure needed to communicate with the spyware, referred to as command-and-control (C2), and the ability to monitor and collect data from the targeted device. In order to install the spyware on a user's device, the CSV must also devise a delivery method, which often means exploiting vulnerabilities in consumer devices and applications to gain access to the device. Each step requires technical expertise, specific understanding of the user's device and applications, and investment in the development of infrastructure and tools.

> CSVs give government customers easy access to spyware in order to surveil an individual — for a price.

Key terms

Vulnerability	A weakness in a device or software that can be exploited to gain access or to perform unauthorized actions on the system.
Common Vulnerabilities and Exposures (CVE)	A public database of disclosed vulnerabilities. Each vulnerability receives a unique identifier in the database, formatted as CVE-YEAR-NUMBER. We use CVE identifiers to refer to publicly disclosed vulnerabilities throughout this report.
Exploit	The process by which a vulnerability is leveraged to gain additional access on a system.
In-the-wild (ITW)	When researchers observe an exploit being used against a device or application for malicious purposes, as opposed to the publication of a description of the exploit or a proof-of-concept of the exploit.
0-day exploit	An exploit that uses a vulnerability that defenders do not yet know exists.

	There is no security patch available to prevent exploitation, nor antivirus signatures that can detect exploitation.
n-day exploit	An exploit that uses a vulnerability that is publicly known.
1-click exploit	An exploit that requires at least one interaction, or click, from the targeted user, such as clicking a link or opening a malicious document.
0-click exploit	An exploit that requires no interaction from the targeted user.
Exploit chain	A combination of exploits designed to get past the defenses of a selected technology, usually to acquire full privileges to the system. To obtain the full privileges needed to install spyware on a device, exploit chains are commonly made up of three types of exploits, remote code execution (RCE), sandbox escape (SBX), and local privilege escalation (LPE).
Remote code execution (RCE)	A type of exploit, usually the first step in an exploit chain, that provides the attacker with the ability to run code on the device. This initial code execution is often used to run the additional steps in the exploit chain.
Sandbox escape (SBX)	A type of exploit, usually the second step in an exploit chain. The initial code execution obtained by the RCE exploit usually runs inside a 'sandbox', or an environment with limited access to the rest of the device. The sandbox escape is used to break out of the sandbox and gain more access to the device.
Local privilege escalation (LPE)	A type of exploit, usually the last step in an exploit chain. After the SBX exploit, the attackers have more privileges than they previously did, but not yet full privileges and access to the device. The local privilege escalation exploits a vulnerability to gain full privileges to the device.

CSVs give government customers easy access to spyware in order to surveil an individual — for a price. Private sector firms have been involved in discovering and selling exploits for many years, but the rise of turnkey espionage solutions is a newer phenomena. CSVs operate with deep technical expertise to offer 'pay-to-play' tools that bundle an exploit chain designed to get past the defenses of a selected device, the spyware, and the necessary infrastructure, all to collect the desired data from an individual's device. Government customers who purchase the tools want to collect various types of data on their highest value targets, including passwords, SMS messages, emails, location, phone calls, and even record audio and video. In order to collect this data, CSVs often develop spyware to target mobile devices.

The groups involved

The development of surveillance technology often begins with the discovery of a vulnerability and ends with a government customer collecting data from spyware installed on a high risk user's device. Broadly speaking, the CSV industry is made up of four primary categories:

1. **Individual vulnerability researchers and exploit developers**: one source for exploits targeting operating systems, browsers, and messaging apps. These individual vulnerability researchers can monetize their work by improving the security of these products (e.g., bug bounty programs or working as defenders) or by enabling attacks (e.g., selling to exploit brokers or directly to CSVs).
2. **Exploit brokers and suppliers**: individuals or companies specialized in selling exploits, located all over the world. While CSVs may have their own in-house employees working on vulnerability research and exploit development, they also supplement them by purchasing bugs and exploits from third parties.
3. **Commercial surveillance vendors (CSV)** also known as Private Sector Offensive Actor (PSOA): CSVs develop and sell spyware as a product, including the initial delivery mechanisms, exploits, the C2 infrastructure, and tools for organizing the collected data.
4. **Government customers**: CSVs sell their spyware to government customers. The government customer selects the target, crafts the campaigns that deliver the spyware, then monitors and commands the spyware implant to collect and receive data from the device.

At every step of the process, brokers can act as intermediaries between sellers, buyers, CSVs, and government customers.

Approaches to developing spyware

CSVs are private technology companies based all over the world. Rather than operating secretly like ransomware and extortion groups, many operate openly. Like any other software product company, they have websites and marketing materials, sales and engineering teams, job openings listed on their websites, publish press releases, and even attend conferences.

The number of CSVs around the globe is impossible to count, with new companies opening each year and existing ones reincorporating under new names. TAG currently tracks approximately 40 CSVs developing and selling exploits and spyware to government customers. In the appendix of this report, we have included a subset of CSVs tracked by Google, their products, and the exploits they have used against consumer devices and applications.

As in the broader software industry, CSVs have taken different approaches to be competitive in the spyware marketplace. CSVs build relationships to provide spyware to government customers, and rely on specialization, collaboration, or acquisitions to offer competitive products. To illustrate the ways CSVs develop, sell, and deliver spyware, we provide an overview of five CSVs, as well as an in-depth description of a sales pitch for a spyware product and examples of campaigns delivering spyware in the following sections.

Cy4Gate and RCS Lab

Acquired but distinct

Founded in Italy in 2014, Cy4Gate develops the "Epeius" spyware targeting Android and iOS systems. In a December 2020 press release, Cy4Gate highlighted their work in "Intelligence Platforms, Cybersecurity and Lawful Interception" for markets in both "Italy and abroad". The release also listed Cy4gate's products, including Epeius. In February 2021, analysis by Citizen Lab and Vice Motherboard linked to Cy4Gate's "Cyber Solutions Portfolio" documents, which described the attributes of the Epeius spyware. TAG has also observed Cy4Gate's Epeius spyware using Android 0-day exploits (CVE-2023-4211, CVE-2023-33106, CVE-2023-33107) against Android devices.

In March 2022, Cy4Gate acquired fellow Italian CSV, RCS Lab, founded in 1993. On their website, RCS Lab claims to have a "Covert Surveillance" solution delivering "highly reliable electronic monitoring solutions". Since being acquired, RCS Lab continues to sell its own spyware, "Hermit", which has been repeatedly used against targets

in-the-wild. TAG has observed RCS Lab campaigns in Italy and Kazakhstan against both iOS and Android devices.

Despite the acquisition, RCS Lab and Cy4Gate have continued to operate independently, maintaining separate operations and spyware products. They appear to maintain distinct customer bases, providing different products to different audiences.

Intellexa

An alliance of capabilities

The Intellexa Alliance, originally based in Cyprus, but now based in Greece, is a prominent example of collaboration among different actors in the CSV industry. Intellexa enriches their intrusion and surveillance products by combining capabilities from different firms together into an "alliance" of CSV vendors, some acquired by Intellexa as subsidiaries, and some close collaborators, each focused on a portion of developing and delivering surveillance capabilities. Intellexa has been widely reported on publicly by TAG, as well as by Amnesty International and the International Consortium of Investigative Journalists (ICIJ).

Rather than a government customer working with each smaller vendor individually, operating as an alliance allows Intellexa to bundle together an end-to-end solution to offer to government customers. Tal Dilian founded the Intellexa Alliance in 2019 bringing together Nexa Technologies, Cytrox, WiSpear, Senpai, and other unnamed entities. (Tal Dilian is also the founder of the surveillance company, Circles Technologies, which was sold in 2014 and merged with NSO Group to form Q Cyber Technologies.)

Cytrox is known for their Predator spyware, which targets both Android and iOS systems. By August 2020, Intellexa was advertising an Android and iOS spyware product as "Nova", but public reporting and security researchers still tend to refer to Intellexa's spyware as Predator. In addition to Cytrox's spyware, WiSpear provides capabilities to intercept WiFi and mobile traffic and Senpai Technologies conducts open source intelligence (OSINT) research to gather information about targets such as their phone number and type of device.

About

The Intellexa Intelligence Alliance was founded by leading providers of intelligence solutions from different disciplines. The goal of the alliance is allow customers to benefit from the unique expertise of each member, while enjoying the synergy
and simplicity of a unified environment.

Founding Members:

nexa TECHNOLOGIES

Nexa Technologies is a key technology provider of Intelligence systems for the Defense and Cyber field. Our core expertise is sensor conception and design to intercept all types of communication alongside big data analytics and unified intelligence centers geared towards merging various sources into one coherent system. Our objective is to assist intelligence agencies and police forces worldwide with their day-to-day investigations. Nexa is headquartered in Paris, France.

WiSpear

WiSpear provides end-to-end intelligence solutions for law enforcement and intelligence agencies. WiSpear's products are based on deep and extensive knowledge of WiFi and RF technologies, years of security and intelligence experience and a long track record in developing best in class WiFi sensors and surveillance systems. WiSpear is headquartered in Limassol, Cyprus.

CYTROX CYBER - INTELLIGENCE - SOLUTIONS

Cytrox provides government agencies with an operational cyber solution for the design, management, and implementation of cyber intelligence operations as well as innovative engines for gathering intelligence from end-point devices and cloud services.

SENPAI

Senpai is a research and development company that specializes in the development of cutting edge open-source intelligence systems.

Screenshot of Intellexa's website (intellexa[.]com) from Aug 2019 via web.archive.org

Negg Group

Organic growth

Negg Group is a relatively small Italian CSV founded in 2013. According to their website, Negg Group is "a research-based company with a focus on cybersecurity, delivering advanced solutions based on dual use technologies to meet companies and government requirements". The company was first publicly exposed in 2017 when Kaspersky Lab revealed that the company had developed a piece of Android malware known as

"Skygofree". Although they had Windows capabilities in 2017, their spyware, called "VBiss", has been primarily used to infect mobile devices via 1-click exploit chains, such as the one described in our blog, or via drive-by download, as described by Kaspersky Lab. TAG has observed Negg Group infection links sent to users in Italy, Malaysia, and Kazakhstan.

Through the years the company has been striving to increase its international presence by exhibiting at international conferences and by expanding its network of partners and resellers outside of Italy.

NSO Group

Sophisticated development

NSO Group is one of the highest-profile CSVs. A surveillance company based in Israel providing "access-as-a-service", Citizen Lab first exposed NSO's Pegasus spyware in 2016. In 2017, Google worked with security company Lookout to uncover the Android version of Pegasus, at that time known as Chrysaor (now both the Android and iOS versions are known as Pegasus). NSO Group develops both the implants and the exploits to deliver them. These are highly sophisticated, such as a 0-click exploit chain developed by NSO Group was observed by Citizen Lab in 2021.

Beginning in 2020, several media organizations conducted an international investigation referred to as the "Pegasus Project" into the use of the Pegasus spyware against high risk users. They reported on government espionage against journalists, opposition politicians, human rights defenders, and others. Pegasus has been linked to the hacking of New York Times journalist Ben Hubbard, the hacking of human rights defenders in Morocco and Bahrain, the targeting of Amnesty International staff, and dozens of other cases. In June 2023 Hanan Elatr Khashoggi, the widow of murdered Washington Post journalist, Jamal Khashoggi, sued NSO Group, saying tools built by NSO Group targeted her devices leading up to her husband's death.

Despite both the US and the EU sanctioning the company in 2021, NSO Group is still operating and selling their spyware. In September 2023, Citizen Lab discovered a 0-day exploit

chain they named "BLASTPASS" against iOS used to deliver Pegasus to an individual working for a civil society organization. In December 2023, TAG discovered a Chrome 0-day, CVE-2023-7024, used by an NSO Group customer.

Variston

Collaboration

Variston is a CSV based in Spain, that claims to be a provider of "tailor made information security solutions". In 2018 Variston acquired Truel IT, an Italian vulnerability research firm which provides "exclusive zero-day capabilities". TAG has connected Variston to the Heliconia exploitation framework, which is used to install spyware on target devices. The Heliconia framework has used both 0-day and n-day exploits against Chrome, Android, iOS, Firefox, and Microsoft Defender.

Variston collaborates with several other organizations to develop and deliver spyware. Protected AE (also known as Protect Electronic Systems), a self-described cybersecurity and forensics company, combines spyware it develops with the Heliconia framework and infrastructure, into a full package which is then offered for sale to either a local broker or directly to a government customer. Variston was founded by Ralf Wegener and Ramanan Jayaraman, who also lead Protected AE. In July 2023, Intelligence Online reported that Variston "has successfully established its cyber-implants in the United Arab Emirates in recent months, by getting gradually closer to Beacon Red, the cyber subsidiary of the part state-owned defence company Edge Group".

Spyware for sale: CSV products

Much of the CSV industry focuses on developing tools to spy on mobile devices. In building these tools, CSVs assemble the different components necessary for their government customers to deliver, install, and communicate with the spyware on a target's mobile device. While each CSV uses different exploit chains, delivery methods, and spyware, they all attempt to provide full service espionage products to their government customers.

Infecting a Mobile Device

When an attacker decides to infect a mobile device there are five key steps to the infection: 1) the initial infection vector is delivered to the target; 2) the target's device is exploited; 3) the spyware is installed; 4) the spyware collects data; and then 5) the spyware exfiltrates or sends the collected data back to the attacker until the spyware is removed from the device. In the following case studies we detail the capabilities of spyware, and use in-the-wild campaigns of CSV customers to illustrate each of these steps.

Introduction to exploit chains

As the security design of devices has progressed, attackers have to use exploit chains rather than a singular exploit to remotely install spyware onto a target's device. An exploit chain is made up of several exploits "chained" or linked together, and often includes three or four different 0-day exploits. Generally the exploits fall into three types: initial remote code execution (RCE), sandbox escape (SBX), and local privilege escalation (LPE). Information leaks are sometimes used to help with the exploitation within the chain as well.

For spyware to be successful, it has to gather data without alerting the user. Government customers want to gather data from a user's device, such as reading messages on their phone or accessing their browser history. However, by design, a single application on a mobile device does not have the privileges needed to access all other applications or data on the device. Each application requires the user to explicitly grant permission to access data, otherwise any downloaded game would be able to access all messages or even the browser history of the device. This barrier between applications is referred to as a sandbox.

An application requesting permission to access data could alert the users to unusual activity, and possibly reveal the presence of the spyware. Instead, CSVs have to exploit vulnerabilities in the device to break out of sandboxes and gain additional privileges. Technology companies have added additional layers of security to increase the difficulty

of exploitation. Installing spyware and accessing all the data on a device requires the highest level of privilege, referred to as "root privilege". Exploit chains often contain local privilege exploits to gain the root privilege needed to install the spyware and access the users' data.

Spyware pricing model

Intellexa's Nova system

In December 2022, the NYT published a 2021 "pitch" document for Predator from Intellexa, showing the cost breakdown of purchasing and using spyware. A more recent commercial offer for 'Nova', Intellexa's offer combining both spyware and a data analysis system, was leaked in August 2022 on a cybercrime forum. These documents include a detailed proposal for the systems, including capabilities and pricing.

The Nova pricing proposal illustrates what professional services CSVs offer to government customers, and at what cost. The proposal is not for a single exploit or spyware implant, but the ability to remotely infect up to ten Android and iOS devices concurrently, along with a system to monitor and organize all data collected by the spyware implants from the targets. Like many other software products, the pricing includes certain guarantees, a maintenance plan, and even training for users.

NOVA Platform
Commercial Proposal

intellexa

2 Price Proposal

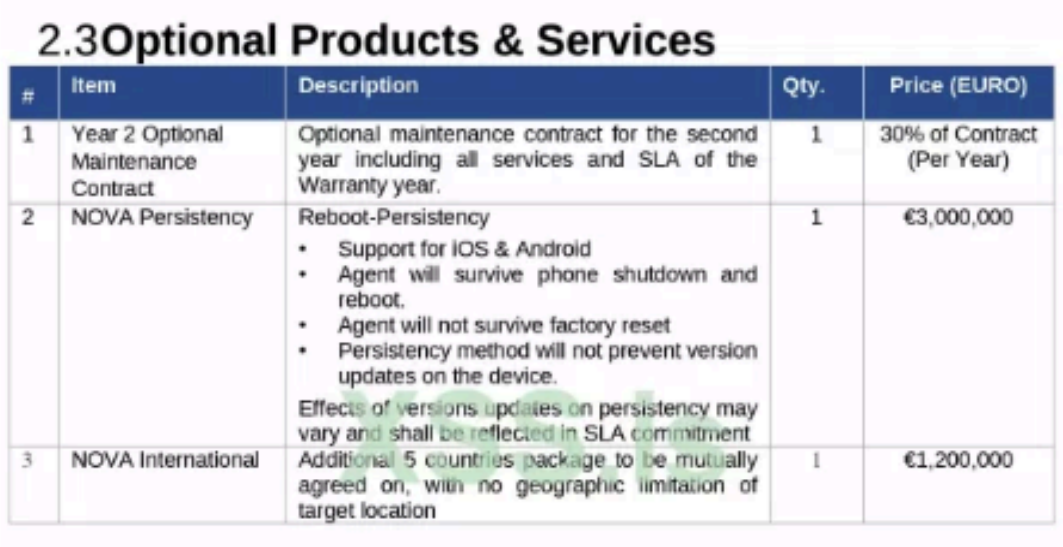
#	Item	Description	Qty.	Price (EURO)
1	**Nova** Remote Data Extraction from Android & iOS Devices & Analytics system	Delivery Studio: Remote 1-Click Browser-based capability to inject Android & iOS payload to mobile devices through link delivery	1	Included
		Supported devices: iOS & Android supported devices (list attached)	1	
		Android Support:* • Android 12 (latest version)*** + 18 months back **iOS Support: *** • iOS latest version*** 15.4.1 + 12 months back	1	
		Agent Concurrency Scope: • 10 Concurrent infections for both OS families (iOS and Android) (i.e. total of 10 infections which may be split between iOS and Android as per the customer sole decision).	10	
		Successful infections magazine: • Magazine of 100 Successful infections.	100	
		Geographical Coverage: Inside the country for local SIM cards on iOS or Android devices.	1	
		Fusion & Analytics system Investigation platform for analysis of all Cyber data extracted by NOVA system. • Cases and targets investigation • Search, filter, analyze and manage cyber data	1	
2	**Hardware & Software**	The entire Nova Suite will be delivered turnkey: • All proprietary software and 3rd party software shall be provided by Intellexa. unless written specifically otherwise under the agreement. • Cloud services, domains and anonymization chain which will be provided and managed by customer.	1	Included
3	**Project Management**	A complete project plan will be provided by INTELLEXA to be approved and coordinated with the customer: • Delivery & Project Plan • Final Design Review • Site Acceptance Testing (Customer site) Technical, operational and methodology	1	Included
4	**Warranty**	Twelve (12) months Warranty as further detailed under section 2.2 below.	1	Included
5	**Price**			**€8,000,000**

In December 2022, the NYT published a 2021 commercial offer for Predator. Later, a more recent commercial offer for 'NOVA' (Intellexa alliance combined spyware and data analysis system) was leaked on the XSS.is cybercrime forum.

Source: Amnesty Security Lab.

For €8 million the customer receives the capability to use a remote 1-click exploit chain to install spyware implants on Android and iOS devices, with the ability to run 10 concurrent spyware implants at any one time. In this example, while the spyware can only run on 10 different devices concurrently, it can be switched between devices or re-infect the same device for up to 100 infections.

Like many software products, additional capabilities can be added for a cost. For example, the baseline price requires that infected devices are within the purchasing customer's country and using that country's SIM cards. For an additional €1.2 million, the customer can infect phones with SIM cards from five additional countries.



2.3 Optional Products & Services

#	Item	Description	Qty.	Price (EURO)
1	Year 2 Optional Maintenance Contract	Optional maintenance contract for the second year including all services and SLA of the Warranty year.	1	30% of Contract (Per Year)
2	NOVA Persistency	Reboot-Persistency • Support for iOS & Android • Agent will survive phone shutdown and reboot. • Agent will not survive factory reset • Persistency method will not prevent version updates on the device. Effects of versions updates on persistency may vary and shall be reflected in SLA commitment	1	€3,000,000
3	NOVA International	Additional 5 countries package to be mutually agreed on, with no geographic limitation of target location	1	€1,200,000

Intellexa Commercial Proposal 2021, originally posted on xss[.]is.

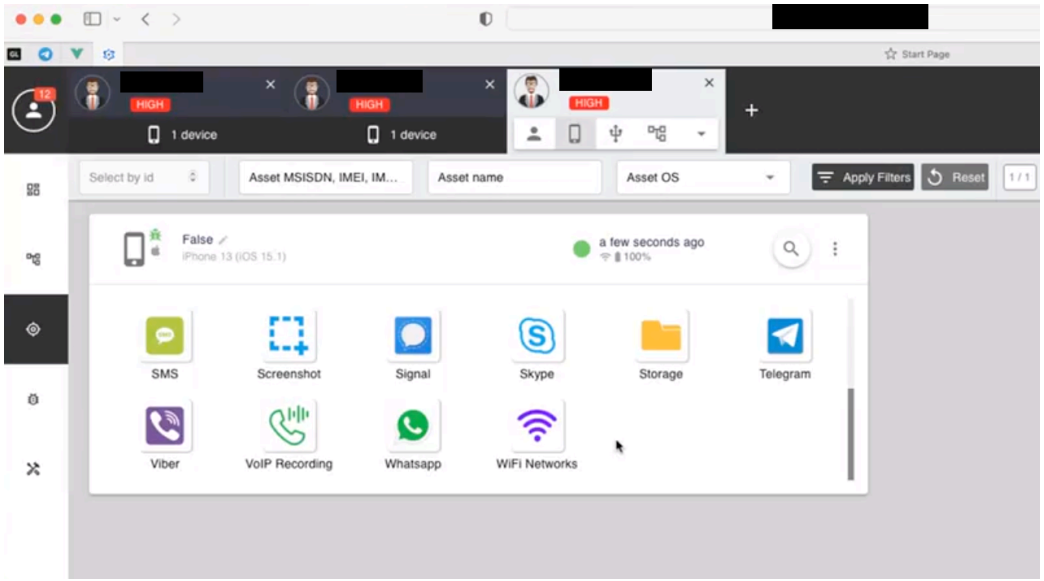
If the spyware remains on the user's phone, it becomes easier to detect, increasing the risk of public exposure. For this reason, "persistence" — the ability for an implant to stay on the phone even after the device is shut down — is not included in the base price but requires an additional €3 million. Many customers choose not to purchase persistence and instead plan to regularly reinfect the target with spyware.

As a part of the €8 million baseline contract, Intellexa guarantees maintenance for one year, meaning that if a 0-day exploit currently used in an exploit chain is patched, the customer will be provided a new exploit.

Intellexa advertises Nova as "turn-key". Once a customer has purchased the product, Intellexa employees will come to the customer facility to configure the hardware and software. The customer will only be responsible for any cloud services or the domains

they wish to use. Intellexa also provides a project plan in coordination with the customer and multiple training sessions on how to use the platform and analyze the collected intelligence.

Once the system is set up, the government customer has an end-to-end infection, spyware, and analysis solution. They can use Intellexa's user interface to build the lure links, send the links through a variety of channels, monitor the status of the exploitation and installation of the spyware agent, and finally command the spyware implant to find and exfiltrate the desired data.



After the spyware has been installed on a target's device, government customers can use a simple web user interface to access the targeted user's data.

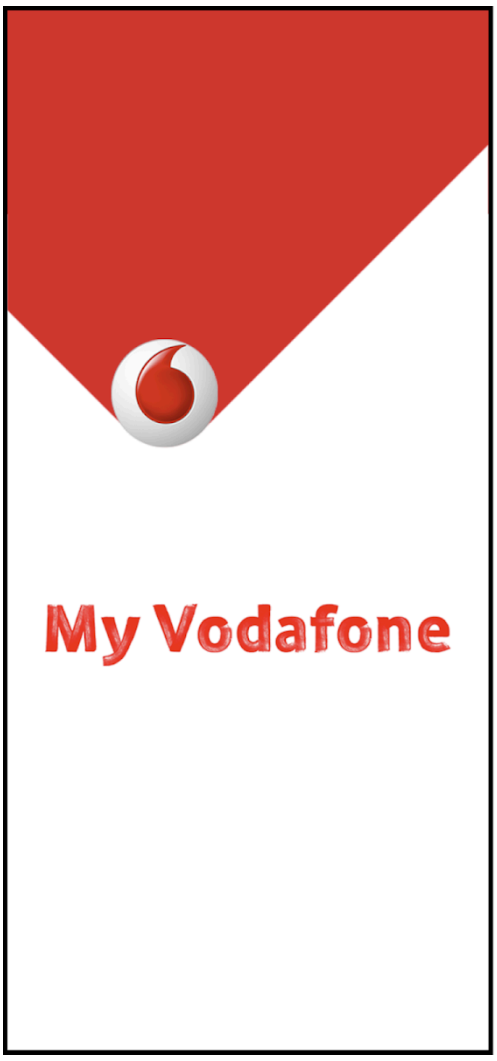
Initial infection vector

RCS Lab's fake apps

RCS Lab uses a combination of initial infection vectors to target mobile users on both iOS and Android devices. In an interesting campaign, RCS Labs worked with internet service providers (ISPs) to convince users to download and install an application. In October 2021, TAG discovered a campaign against victims located in Italy and Kazakhstan that delivered both iOS and Android applications impersonating legitimate apps, which used exploits to gain access to the target's data.

iOS campaign

The iOS application impersonated the official application of Vodafone, a multinational telecommunications company. TAG believes the attacker asked Vodafone to disable the target's mobile data connection, and then sent a lure SMS to the target. The SMS pretended to be the official ISP and claimed that in order to restore mobile data connectivity, the target had to install a fake application, and included a download link. In addition to the fake Vodafone application, RCS Lab used applications impersonating legitimate messaging apps.



Screenshot of fake Vodafone application.
Source: Project Zero

The iOS application contained a series of different privilege escalation exploits and a minimal spyware implant responsible for exfiltrating interesting files from the device, such as the WhatsApp database. The application included many different exploits to account for different iPhone models. There were six different privilege escalation exploits included in the app, including four n-days based on publicly published exploits,and two 0-days. Both the 0-days, CVE-2021-30883 and CVE-2021-30983, are local privilege escalation vulnerabilities in the IOMobileFrameBuffer, a kernel extension in iOS.

iOS Privilege Escalation Exploits in the RCS Lab application

CVE	Description
CVE-2018-4344	referred to and publicly known as LightSpeed (n-day)
CVE-2019-8605	referred to as SockPort2 and publicly known as SockPuppet (n-day)
CVE-2020-3837	referred to and publicly known as TimeWaste (n-day)
CVE-2020-9907	referred to by the malware as AveCesare (n-day)
CVE-2021-30883	referred to by the application as Clicked2, fixed in October 2021 (0-day at time of exploitation)
CVE-2021-30983	referred to by the application as Clicked3, fixed in December 2021 (0-day at time of exploitation)

After the application was installed on an iPhone, the attackers only needed a single privilege escalation exploit to obtain privileges for the implant to collect personal data to send back to the attackers' server. In this case an initial remote code execution exploit was not needed because the application provided the initial code execution, and the attackers could proceed directly to the privilege escalation exploit.

Android campaign

For Android devices, RCS Labs also used installation of a fake application as their initial infection vector. However, this required the victim to enable installation of applications from unknown sources, as the applications were never available in the Google Play Store. It's likely that the message instructing the user to install the app also directed the user to enable installation of apps from unknown sources on their device.

The initial sample discovered by TAG had been uploaded to VirusTotal and was disguised as a legitimate Samsung app. Lookout discovered another sample used in Kazakhstan in April 2022, which pretended to be a legitimate app from Oppo, an Android manufacturer. Since then, TAG has discovered many additional variations of apps, most of them pretending to be an app from Android manufacturers, an ISP, or a messaging application. When the user launches the app, a legitimate website related to the app's icon is displayed.

Fake application disguised as a legitimate Samsung app.
Source: Google blog

Unlike the iOS application, the Android application does not include the exploits in the applications. Instead, the Android applications contact a remote C2 server to receive the modules that it should run after install, including the exploits. At this time, TAG has not been able to examine modules from the server, and it remains unclear which exploits were used.

0-click exploit chain

NSO's FORCEDENTRY

Users, especially high risk users, have become more security conscious over time and often follow best practices such as not clicking links or not installing apps from places other than an official app store. This requires CSVs to innovate, developing 0-click exploits in consumer devices or applications. A 1-click exploit requires at least one interaction from the target, such as clicking a link, opening a malicious document, or running a program. The need for the user to take any action introduces uncertainty for the CSV, as a wary user may not click on the most well-designed lure,

preventing the delivery of the spyware. A 0-click exploit removes this uncertainty, as an attack can succeed without any actions from the targeted user.

In 2021, Citizen Lab reported on a 0-click exploit chain developed by NSO Group used to target a Saudi Arabian human rights defender. This 0-click exploit chain, called FORCEDENTRY, remotely and surreptitiously installed the Pegasus spyware onto an iPhone. Two of the exploits in the chain were recovered: the initial remote code execution vulnerability (CVE-2021-30860) and the sandbox escape (CVE-2021-31010), but at least one more vulnerability, the local privilege escalation, would have been required in order to have the full access to the device required for the spyware. Citizen Lab shared FORCEDENTRY with Google Project Zero, which published a deep dive analysis of the exploit chain.

Initial Remote Code Execution: CVE-2021-30860

In iOS 14, Apple released a new exploit mitigation, called "BlastDoor", to make it more difficult for attackers to develop 0-click exploits against iMessage. NSO Group found a way around this new mitigation via GIFs. GIFs, or more specifically files with the `.gif` file extension, were processed in a separate process, `IMTranscoderAgent`, which was less restrictive than BlastDoor. Additionally, once a GIF was moved into `IMTranscoderAgent`, the file was re-processed, this time without its file extension, to determine its file type and to decide how to parse it. As there were more than 20 different supported file types, an attacker could use a vulnerability in any one of these types of file parsing functions, greatly expanding the potential attack surface.

To take advantage of this, NSO Group used a PDF file masquerading as a GIF. This caused the file to be moved from BlastDoor into `IMTranscoderAgent` and then be processed by the PDF parser. FORCEDENTRY then exploited CVE-2021-30860, an integer overflow vulnerability within the CoreGraphics PDF parser and gained code execution.

What is an integer overflow vulnerability?

An integer overflow vulnerability is a type of memory corruption vulnerability that occurs when the space assigned to store a number is too small to store the number assigned to the space. For example, let's say that you only assign 2 digits to store a number. The maximum integer that can be stored in 2 digits is 99. So if you do `99+1=100`, you overflow the space. Instead of now having `100` you'd have `00` because you only have two digits to store this number.

Integer overflows can be used to trigger memory overflows, allowing an attacker to overwrite an area in memory beyond what the developer initially intended, leading to arbitrary code execution.

Sandbox escape: CVE-2021-31010

At this point in the attack, FORCEDENTRY had code execution within `IMTranscoderAgent`. While `IMTranscoderAgent` has more access to data and other processes than BlastDoor, it is still itself a sandbox. To install the Pegasus spyware, FORCEDENTRY needed to access more privileges.

To escape the `IMTranscoderAgent` sandbox, FORCEDENTRY used `XPC`, iOS's inter-process communication mechanism, to trigger a logic vulnerability, CVE-2021-31010. `XPC` allows a process to call methods on an object in another process. FORCEDENTRY used this to get code execution in the `CommCenter` process, therefore breaking out of the `IMTranscoderAgent` sandbox. Next, FORCEDENTRY attempted to contact the C2 server to receive the next exploit in the chain.

No further stages of the exploit for analysis were obtained, but there would have had to have been at least one more exploit in the FORCEDENTRY exploit chain in order to install Pegasus and collect the target's data.

Vendor response

Just like attackers have to adjust when vendors release new mitigations, vendors work to release new mitigations to disrupt attackers' current techniques. After the discovery of FORCEDENTRY, in iOS 14.8.1, Apple further restricted the available file formats processed by `IMTranscoderAgent`. In iOS 15, they removed the GIF processing from `IMTranscoderAgent` and put it within the BlastDoor sandbox, breaking the FORCEDENTRY exploit chain. To mitigate against the sandbox escape technique, in iOS 15.1 Apple significantly reduced the abilities of one of the objects in `XPC`, `NSExpressions`, that had been abused by FORCEDENTRY.

Modular framework

Variston's Heliconia

Variston developed the Heliconia exploitation framework in order to deliver exploits and install their spyware implant, BridgeHead, on a range of different devices. Using a single framework across all of their platforms allows them to modularize their product and re-use code from one platform to the other. For each particular platform, the requisite individual exploits are loaded into the framework and used against the target device.

TAG has observed multiple campaigns using the Heliconia framework targeting devices including Chrome and Android devices, and variants that support Windows exploitation. In July 2021, Google received anonymous submissions to the Chrome vulnerability reporting program (VRP) that contained the Heliconia framework with various exploits. The exploitation framework, detailed in a blog post, included code capable of deploying exploits for Chrome, Windows Defender, and Firefox on Windows computers. Although the vulnerabilities were patched at the time of the submission to the Chrome VRP, TAG assessed the vulnerabilities were likely used as 0-days at the time of the campaigns. The project included a pre-commit cleaning script that exposed the company name behind the framework, Variston.

TAG then identified in-the-wild campaigns using this exploitation framework to target mobile devices in Indonesia

and the United Arab Emirates with different exploits, including both 0-days and n-days.

```
strings = GetStrings(path)

badStrings = ['heliconia', 'heliconia-charlotte',      # project name
              'freezer', 'majinbuu', 'janemba',        # developer names
              'variston'                               # company name
              ]
```

Pre-commit script showing company name

Android campaign

In December 2022, TAG discovered a campaign using one-time links, or links that only work once, to target Android devices located in the United Arab Emirates. The Heliconia framework contained an exploit chain that chained together six vulnerabilities to target Samsung devices. The exploit chain ultimately delivered a fully featured Android spyware suite written in C++ , called "BridgeHead", and also includes libraries for decrypting and capturing data from various chat and browser applications. However, at the end of the process, the user was redirected to Stack Overflow, a popular benign website, with no indication that spyware had been installed.

Four of the six vulnerabilities used in the chain were 0-days at the time of the campaign. The remaining two vulnerabilities had patches available, but due to challenges with patching timelines, they functioned against user devices as 0-days. The sandbox escape, CVE-2022-3038, had been patched four months earlier in Chrome 105. This meant that the exploit chain would not work against the most up-to-date versions of Google Chrome at the time. However, the attackers ensured that the link was opened in Samsung Browser rather than in Chrome. Samsung Browser is built on top of Chromium, but is often a few versions behind the most current version. At the time of discovery, Samsung Browser was on Chromium version 102 and therefore CVE-2022-3038 was unpatched and functioned like an 0-day on the Samsung Browser. A local privilege escalation vulnerability in the Mali GPU driver, CVE-2022-22706, had been fixed by Arm almost a year earlier in January 2022. However, as many Android devices had not yet incorporated the patch, it functioned as an 0-day on Samsung devices.

Exploits Used in Android Campaign

CVE	Description
CVE-2022-4262	type confusion vulnerability in Chrome fixed in December 2022 (0-day at time of exploitation)
CVE-2022-3038	sandbox escape in Chrome fixed in August 2022, in version 105 and found by Sergei Glazunov in June 2022 (Unpatched in Samsung Browser at the time of exploitation)
CVE-2022-22706	vulnerability in Mali GPU Kernel Driver which grants the attacker system access fixed by Arm in January 2022 (At the time of exploitation, the latest Samsung firmware had not included a fix for this vulnerability)
CVE-2023-0266	race condition vulnerability in the Linux kernel sound subsystem reachable from the system user and that gives the attacker kernel read and write access (0-day at time of exploitation)
CVE-2022-22706	kernel information leak 0-days impacting the Mali GPU Kernel Driver (0-day at time of exploitation)
CVE-2023-0266	kernel information leak 0-days impacting the Samsung Kernel (0-day at time of exploitation)

iPhone campaign

Variston continues to develop the Heliconia framework. In March 2023, TAG discovered a campaign delivered to iPhones located in Indonesia. The campaign began with a link delivered by SMS, and at the end of the process, the victim was redirected to a news article on the website for Pikiran Rakyat, an Indonesian newspaper.

The exploit chain worked against iPhone models running iOS versions 16.3.0 and 16.3.1, and used the Heliconia framework to chain three 0-day exploits. While TAG was not able to capture the spyware delivered at the end of the exploit chain, it is likely an implant with similar capabilities to the Android version of BridgeHead.

Exploits used in iPhone campaign

CVE	Description
CVE-2023-28205	a use-after-free vulnerability in Safari used to get initial remote code execution (0-day at time of exploitation)
CVE-2023-32409	an out-of-bounds access in `WebGPU` to escape the sandbox (0-day at time of exploitation)
CVE-2023-28206	an out-of-bounds access in `IOSurfaceAccelerator` to elevate privileges (0-day at time of exploitation)

Data collection

Cy4Gate's Epeius

Cy4Gate develops a spyware implant named Epeius with the package name `com.android.systemapn`. The implant is a simple but modular Android application with different plugins that illustrate the types of data collected by spyware. We have seen Epeius is delivered and installed via exploit chains, and each installed implant contains a unique Agent ID identifying the target. Once installed, Epeius has multiple plugins which can be used depending on what information the attacker wants to collect from the target device.

TAG has observed 18 distinct Epeius plugins, providing different functionalities. When the spyware is first delivered to the device, the implant is bundled with an initial set of encrypted plugins, which are decrypted then loaded once the spyware begins to run.

One of the plugins, `plglpe`, uses exploits to escalate local privileges. The plugin uses ECDH encrypted communications to send system information, such as the Android version and GPU driver version, to the attacker's C2 server, and then receives back the correct LPE exploit for the specific device. Epeius uses two different frameworks for exploits, potentially signaling that they get their exploits from two different providers: "YodaRoot" and "DF1".

To exfiltrate, or send data collected by the implant back to the attacker's C2 server, Epeius uses the `plgpucexfiltrator` plugin. This plugin exfiltrates data stored in the plgevidence plugin back to the C2 server using secure websockets. The data is AES encrypted with a random key which is sent back to the C2 using a RSA public key hardcoded into the implant.

Additional plugins can be remotely delivered and activated on-demand via the C2, depending on the requirements of the attacker. In addition to `plglpe` and `plgpucexfiltrator` plugins, we observed 16 other plugins which primarily collect and store data on the device. In order to collect the various types of private data, the spyware obtains root access, the highest privileges on the phone. The attackers then have access to all of the data on the phone. For example, to gather messages the attacker has access to messaging data from all apps, instead of exploiting a security weakness in each individual app, such as WhatsApp, Signal, Telegram, or Gmail.

CSV spyware like Epeius can be used to monitor and collect a wide range of personal information, including the location of the device, activity on social media, private calls, or audio recordings of the phone's surroundings. The modular nature of Epeius allows customers to choose what kind of data to collect and exfiltrate.

Plugin name	Function
`plgroot`	Checks to see if the phone is already rooted or unlocked
`plglocation`	Collects GPS location information
`plgfrida`	Injects code into other applications
`plgmic`	Records the microphone
`plgdb`	Exports database of popular applications like Calendar, Signal, WhatsApp, and Telegram
`plggmail`	Collects emails from GMail
`plgsysinfo`	Collects system information
`plgnotification`	Intercepts notifications from messaging applications
`plgvoip`	Records voice-over-IP (VoIP) calls
`plgcamera`	Records camera
`plgpasswords`	Collects saved passwords
`plgfilesystem`	Interacts with the filesystem
`plgscreenshot`	Takes and saves screenshots
`plgaccessibility`	Takes screenshots from browsers using accessibility API
`plgevents`	Sets certain actions to occur on certain events. (Example: Record mic during a phone call to a specified number)
`plgevidence`	Stores the “evidence” and data collected by other plugins

Spyware targeting Google products

CSVs pose a threat to Google users, and Google is committed to disrupting that threat and keeping our users safe. Every time Google and fellow security researchers discover and patch vulnerabilities used by CSVs, it not only protects users, but prevents CSV and their customers from using those exploits.

CSVs are behind nearly half of known 0-day exploits targeting Google products. From mid-2014 through 2023, security researchers have discovered 72 in-the-wild 0-day exploits affecting Google products, including Chrome and the Android ecosystem. We include vulnerabilities targeting Android components or our OEM partners. TAG attributes 35 of these 0-day exploits targeting Google products to CSVs. For additional information, see the Appendix.

This is a lower bounds estimate, as it reflects only known 0-day exploits. The actual number of 0-day exploits developed by CSVs targeting Google products is almost certainly higher, after accounting for exploits used by CSVs that have not been detected by researchers, exploits where attribution is unknown, and cases where a vulnerability was patched before researchers discovered indications of exploitation in-the-wild.

For example, in 2022, TAG analyzed an exploitation framework produced by the spyware vendor Variston. At the time of analysis, the framework exploited n-day vulnerabilities in Chrome, Firefox and Microsoft Defender. However, based on TAG's research, we suspect Variston or its customers used these exploits before the vulnerability was patched in a software update, as 0-days in-the-wild.

Over time, we have observed an accelerating cadence in the discovery of 0-day exploits, including those attributed to CSVs. From 2019 to 2023, TAG alone discovered 53 0-day exploits, including 33 that were developed by CSVs. As we have discussed in the past, the growth in 0-day exploit discoveries is not attributable to any one factor, and a mix of security improvements and regressions likely influence how many 0-days researchers discover each year. One important factor is changing norms around public disclosure among technology vendors, with more vendors noting in their advisories when a bug was exploited in the wild. We view this shift as a positive one, and it has helped shed light on the extent to which the commercial surveillance industry is thriving and putting users at risk.

Making it harder for CSVs to target Google users

Often when CSVs sell a product to government customers, they are selling a guarantee that the spyware implant will work against a targeted device, and the customer will maintain access to that device for a certain time period. However, this process depends on exploit chains continuing to work against targeted devices and applications. Exploit chains are expensive and hard to develop. Each time Google and fellow security researchers discover and disclose new bugs, it causes friction for CSVs and costs them development cycles.

When we discover and patch vulnerabilities used in exploit chains, it not only protects users, but prevents CSVs from meeting their agreements to customers, preventing them from being paid, and increasing their costs to continue operating.

In one recent case, it took Intellexa weeks to recover from the setback of Chrome patching vulnerabilities exploited in one of their exploit chains. On April 14, 2023, Chrome released patches for CVE-2023-2033 and CVE-2023-2136, which Intellexa were using in a 0-day exploit chain to install their spyware. Following the Chrome security update, TAG saw a dip in activity by Intellexa's customers for over 40 days, followed by a spike in activity at the end of May when Intellexa released a new 0-day exploit for the next version of Chrome. It took Intellexa roughly 45 days to develop and deploy a new 0-day exploit for Chrome 113. TAG quickly discovered the new exploit and Chrome released a fix for the new 0-day within four days. Intellexa's customers were only able to use the new exploit for less than a week, as Chrome patched the bug, tracked as CVE-2023-3079, in an update released on June 5. By identifying and patching vulnerabilities, security researchers are able to break the exploit chains attackers rely on, causing disruptions and preventing attacks against users.

Google continues to invest in detecting and defending against these threats to not only detect and disrupt existing operations quickly, but to make it as difficult as possible for attackers to return and conduct new operations. We are striving to normalize transparency around actively exploited vulnerabilities across the industry by committing to publicly disclose when we have evidence that vulnerabilities have been exploited, and by maintaining a public repository of technical details on 0-days that have been actively exploited, arming defenders with the same information as the attackers.

As long as there is a demand for surveillance capabilities, there will be incentives for CSVs to continue developing and selling tools, perpetrating an industry that harms high risk users and society at large.

Proliferation of capabilities

As long as there is a demand for surveillance capabilities, there will be incentives for CSVs to continue developing and selling tools, perpetrating an industry that harms high risk users and society at large.

CSVs enable the proliferation of dangerous hacking tools worldwide. Surveillance tools are expensive to develop and maintain, and the CSV market allows any entity to "pay-to-play" and have a full remote surveillance capability instead of (or in addition to) developing the tools themselves.

The ability to acquire espionage capabilities off the shelf increases the likelihood of harm against users. The ability to purchase an end-to-end surveillance capability from CSVs normalizes the use of spyware against high risk users. Providing guaranteed access to certain targeted devices shifts the burden of the cost and reputational risk of the exposure of these tools from the government customer to the CSV. This shifting of cost may increase the likelihood the tools will be used. As government entities buy off-the-shelf capabilities from the CSV industry, the use of spyware becomes increasingly normalized.

CSVs pivot and persist

Exposure through public reporting, and even direct legal action, are not enough to curb the activities of CSVs. The activities of NSO Group, for example, were reported on publicly as early as 2015, they have been added to the US Entity List, and technology companies have taken direct legal action against the group (2019 by Meta [1, 2] and 2021 by Apple), but the group continues to sell its tools. NSO Group continues to operate, and is under new leadership as of May 2023.

In order to avoid public scrutiny, CSVs may change their names multiple times. For example, Citizen Lab has tracked how the Israeli CSV, tracked as Candiru, has transformed over time.

Company name	Date of registration	Possible meaning
Saito Tech Ltd. (סאייטו טק בעיימ)	2020	"Saito" is a town in Japan
Taveta Ltd. (טאבטה בעיימ)	2019	"Taveta" is a town in Kenya
Grindavik Solutions Ltd. (גרינדוויק פתרונות בעיימ)	2018	"Grindavik" is a town in Iceland
DF Associates Ltd. (ד. אף אסוסיאייטס בעיימ)	2017	?
Candiru Ltd. (קנדירו בעיימ)	2014	A parasitic freshwater fish

Table 1: Candiru's corporate registrations over time

Source: Citizen Lab

In response to direct legal action, CSVs are forced to operate quietly, or to shut down operations. In one case, the French CSV Nexa Technologies, a founding member of the Intellexa Alliance, removed themselves from all public mentions of Intellexa in response to indictments. In June 2021 four executives were indicted by the crimes against humanity and war crimes unit of the Paris Judicial Court for "complicity in acts of torture" by selling surveillance software to the Libyan and Egyptian governments. While Nexa Technologies continues to operate, they now have a much lower profile. Gamma, a Munich-based spyware company that develops FinFisher declared insolvency in February 2022 amid an ongoing investigation into its business dealings. The controversial firm was selling surveillance spyware to repressive regimes to target dissidents, human rights defenders, and journalists. However, the firm may still be active, and may return with different tools or under different names.

While CSVs pivot and persist in their activities, bringing public scrutiny to their actions causing disruptions, delays, and even temporary cessations to their activity. This both prevents attacks against users, and makes it harder for CSVs to advertise and sell their products. In addition to public scrutiny, we welcome the actions of governments to contain the proliferation of dangerous tools and capabilities which threaten the safety of the Internet ecosystem, and threatens the trust on which a vibrant and inclusive digital society depends.

Call to action

We believe it is time for government, industry and civil society to come together to change the incentive structure which has allowed these technologies to spread. In a positive sign, several domestic and international initiatives have launched in the past two years, but these must be built upon and converted to sustained action.

In August 2023, U.S. President Biden issued an Executive Order limiting operational use by the U.S. government of commercial spyware that poses risks to national security or has been misused by foreign actors to enable human rights abuses around the world. This is a welcome step, and we encourage the U.S. to share information about its implementation. Greater understanding of steps the U.S. is taking to counter the threat, and releasing public analysis of risks posed by vendors, will help build an international response.

We also welcome steps taken by the U.S. government in applying sanctions to NSO Group, Candiru, and Intellexa, and we believe other governments should consider expanding these restrictions. The U.S. should also consider ways to foster greater transparency, including setting heightened transparency requirements for the domestic surveillance industry, and setting an example to other governments by reviewing and disclosing its own historical use of these tools. Additionally, the U.S. government should contemplate imposing further sanctions to limit spyware vendors' ability to operate in the U.S. and receive U.S. investment. The harms from this industry are amply evident by this point, and we believe they outweigh any benefit to continued use.

Movement towards creating regulation against the misuse of commercial spyware is increasing, and that momentum must be maintained.

Movement towards creating regulation against the misuse of commercial spyware is increasing, and that momentum must be maintained. In March 2023, at the Summit for Democracy, 35 nation states endorsed "Guiding Principles on Government Use of Surveillance Technologies" to ensure responsible use of surveillance technology. In addition, the governments of Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the UK and the US issued a Joint Statement on efforts to counter the proliferation and misuse of commercial spyware. The governments committed to establishing procedures for use of commercial spyware by their own governments, prevent the export to users likely to use them for malicious cyber activity, and to drive reform of the industry. These commitments are promising developments, but concrete action so far has been limited. We encourage other governments to fulfill their pledge by following the U.S. government's example, and banning commercial spyware that has been misused to enable human rights abuses around the world.

Finally, we urge the U.S. government to lead a diplomatic effort to work with the governments of the countries who harbor problematic vendors, as well as those who employ these tools, to build support for measures that limit harms caused by this industry. With the majority of CSV firms marketing their capabilities across national borders, any one government's ability to meaningfully impact this market is limited. Only through a concerted international effort can this serious risk to online safety be mitigated.

Google's work to protect users

Google is investing heavily to counter serious threats to our users. In the modern world, we must be able to trust the devices we use every day and ensure that adversaries do not have access to exploits. While we continue to fight these threats on a technical level, the providers of these capabilities operate openly. Google is committed to leading the industry in detecting and disrupting these threats.

Across all Google products, we incorporate industry-leading security features and protections to keep our users safe. Google's Safe Browsing is an industry-leading service to identify unsafe websites across the web and notify users and website owners of potential harm. On Gmail, we provide security precautions to prevent spoofing, phishing, and spam. To protect high risk user accounts, we offer the Advanced Protection Program (APP), which is our highest form of account security. For Android and Chrome, through their entire development lifecycles, we subject the products to a rigorous security program, and believe all software products should be secure by design. We have also built additional tools to prevent successful attacks on devices that run Android once those devices are in users' hands. For example, Google Play Protect, our built-in malware protection for Android, leveraging Google's advanced AI, continuously scans devices for potentially harmful applications.

We've also created a comprehensive security response process to respond to incidents. Furthermore, when Google discovers malicious activities, we not only take steps to protect users, but also disclose that information publicly to raise awareness and help the entire ecosystem, in line with our historical commitment to openness and democratic values.

In order to address the harms of the CSV industry, Google collaborates with other technology companies in order to detect and address exploitation of vulnerabilities in-the-wild. We also seek to reduce the risk of vulnerabilities and protect researchers. We support measures to shorten the vulnerability identification and mitigation cycle while addressing the most widely exploited vulnerabilities. TAG's policy is to quickly report vulnerabilities to vendors. Project Zero is a critical component of this strategy, promoting transparency and more timely patching of vulnerabilities. Google's vulnerability rewards program (VRP) rewards researchers millions of dollars for their contributions in securing our devices and platforms. We also provide research grants to security researchers to help fund and support the research community. This is all part of a larger strategy to keep Google products and users, as well as the Internet at large more secure.

About the authors

Threat Analysis Group

Google's Threat Analysis Group (TAG) is responsible for countering threats to Google and our users from government-backed attackers, targeted 0-day exploits, coordinated information operations (IO), and serious cybercrime networks. We apply our intelligence to improve Google's defenses and protect users.

Special thanks to Google Jigsaw for partnering with high risk users who allowed us to share their stories.

Appendix: CSV Products and Known 0-day Exploits

Name	Aliases	Spyware Products	0-days targeting Google products	0-days targeting other products
Candiru	remora-tech, Candiru, cyna-tech, Nerfwall, tavetasolution	DevilsTongue	CVE-2021-21166 Google Chrome CVE-2021-30551 Google Chrome CVE-2022-2294 Google Chrome CVE-2022-3723 Google Chrome CVE-2023-5217 Google Chrome	CVE-2018-5002 Adobe Flash [1, 2] CVE-2021-31979 Microsoft Windows CVE-2021-33742 Microsoft Internet Explorer CVE-2021-33771 Microsoft Windows
Cy4Gate		Epeius	CVE-2021-22600 Linux kernel, exploited against Android CVE-2021-25394 Samsung MFC charger driver, exploited against Android CVE-2023-4211 Arm Mali GPU, exploited against Android CVE-2023-33106 Qualcomm Adreno GPU, exploited against Android CVE-2023-33107 Qualcomm Adreno GPU, exploited against Android	
DSIRF		Subzero		CVE-2021-28550 Adobe Reader CVE-2021-31199 Microsoft Windows CVE-2021-31201 Microsoft Windows

				CVE-2021-36948 Microsoft Windows CVE-2022-22047 Microsoft Windows
Intellexa	Cytrox, Nexa Technologies, WiSpear	Nova, Triton, Helios, ALIEN (stager) PREDATOR (Android/iOS)	CVE-2019-2215 Android kernel CVE-2021-1048 Google Android CVE-2021-1905 Qualcomm Adreno GPU, exploited against Android CVE-2021-1906 Qualcomm chipsets, exploited against Android CVE-2021-28664 Arm Mali GPU, exploited against Android CVE-2021-39793 Arm Mali GPU, exploited against Android CVE-2021-30554 Google Chrome CVE-2021-37973 Google Chrome CVE-2021-37976 Google Chrome CVE-2021-38000 Google Chrome CVE-2021-38003 Google Chrome CVE-2022-3075 Google Chrome CVE-2023-2033 Google Chrome CVE-2023-2136 Google Chrome CVE-2023-3079 Google Chrome	CVE-2023-41991 Apple iOS CVE-2023-41992 Apple iOS CVE-2023-41993 Apple iOS
Negg		Vbiss	CVE-2021-28663 Arm Mali GPU, exploited against Android CVE-2022-3723 Google Chrome	CVE-2022-42856 Apple Safari

			CVE-2022-4135 Google Chrome	
NSO Group	Q-Cyber, Circles	PEGASUS (Android / iOS)	CVE-2019-2215 Android kernel CVE-2023-7024 Google Chrome	CVE-2016-4655 Apple iOS CVE-2016-4656 Apple iOS CVE-2016-4657 Apple iOS CVE-2019-3568 Facebook WhatsApp CVE-2021-30860 Apple iOS CVE-2021-31010 Apple iOS CVE-2023-41061 Apple iOS CVE-2023-41064 Apple iOS Exploits without publicly confirmed CVE's: KISMET, exploited against Apple iOS
PARS Defense				CVE-2023-42916 Apple WebKit CVE-2023-42917 Apple WebKit
QuaDream		REIGN		Exploits without publicly confirmed CVE's: ENDOFDAYS, exploited against Apple iOS
RCS Lab		Hermit		CVE-2021-30883 Apple iOS kernel CVE-2021-30983 Apple iOS kernel

Variston	Variston IT, TruelIT, Protected.AE, EdgeGroup	Heliconia (exploitation framework), BridgeHead	CVE-2022-4262 Google Chrome CVE-2023-0266 Google Android CVE-2023-21492 Samsung Android CVE-2023-26083 Arm Mali GPU, exploited against Android CVE-2023-33063 Qualcomm Adreno GPU, exploited against Android	CVE-2022-26485: Mozilla Firefox CVE-2023-28205 Apple WebKit CVE-2023-28206 Apple iOS CVE-2023-32409 Apple WebKit
Wintego Systems			CVE-2019-2215 Android kernel CVE-2021-0920 Google Android CVE-2022-2856 Google Chrome	